

配置VPN电话并排除故障

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[ASA 配置](#)

[CUCM 配置](#)

[故障排除](#)

[要收集的数据](#)

[常见问题](#)

[更新ASA自签名身份证书](#)

[ASA选择椭圆曲线\(EC\)密码](#)

[DTLS连接失败](#)

[证书更新后电话无法连接到ASA](#)

[电话无法通过DNS解析ASA URL](#)

[电话不启用VPN](#)

[电话注册但无法显示呼叫历史记录](#)

[相关信息](#)

简介

本文档介绍如何配置和排除Cisco IP电话和Cisco Unified Communications Manager的VPN电话功能故障。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科统一通信管理器 (CUCM)
- 思科自适应安全设备(ASA)
- AnyConnect虚拟专用网络(VPN)
- 思科IP电话

使用的组件

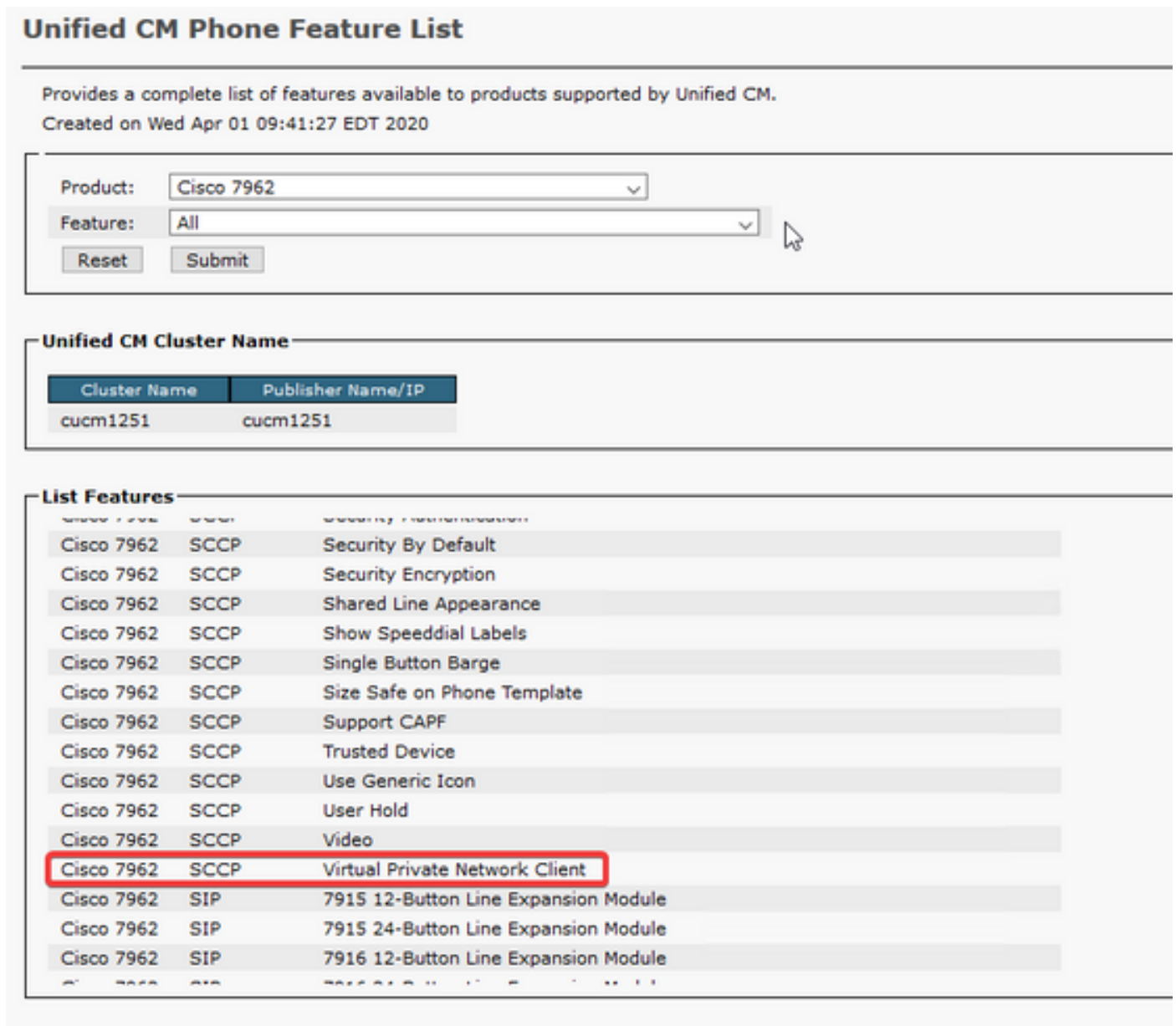
- 8861 14-0-1-0101-145
- ASAv 9.12(2)9

- CUCM 11.5.1.21900-40

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文中的测试环境包括8861、ASA和CUCM 11.5.1，但您可以使用这些产品的许多不同版本。您必须检查CUCM上的Phone Feature List（电话功能列表），以确保您的电话型号支持VPN功能。要使用电话功能列表，请在浏览器中访问您的CUCM发布者，然后导航至Cisco Unified Reporting > Unified CM电话功能列表。生成新报告，然后在下拉列表中选择您的电话型号。接下来，您需要搜索虚拟专用网络客户端的“列表功能”部分，如图所示：



Unified CM Phone Feature List

Provides a complete list of features available to products supported by Unified CM.
Created on Wed Apr 01 09:41:27 EDT 2020

Product: Cisco 7962
Feature: All
Reset Submit

Unified CM Cluster Name

Cluster Name	Publisher Name/IP
cucm1251	cucm1251

List Features

Product	Protocol	Feature Name
Cisco 7962	SCCP	Security By Default
Cisco 7962	SCCP	Security Encryption
Cisco 7962	SCCP	Shared Line Appearance
Cisco 7962	SCCP	Show Speeddial Labels
Cisco 7962	SCCP	Single Button Barge
Cisco 7962	SCCP	Size Safe on Phone Template
Cisco 7962	SCCP	Support CAPF
Cisco 7962	SCCP	Trusted Device
Cisco 7962	SCCP	Use Generic Icon
Cisco 7962	SCCP	User Hold
Cisco 7962	SCCP	Video
Cisco 7962	SCCP	Virtual Private Network Client
Cisco 7962	SIP	7915 12-Button Line Expansion Module
Cisco 7962	SIP	7915 24-Button Line Expansion Module
Cisco 7962	SIP	7916 12-Button Line Expansion Module

配置

VPN电话要求您在ASA和CUCM上配置正确。您可以先从任一产品开始，但本文档首先介绍ASA配置。

ASA 配置

步骤1.检验ASA是否已获得许可，可支持AnyConnect for VPN电话。ASA上的**show version**命令可用于验证Anyconnect for Cisco VPN Phone是否已启用，如以下代码片断所示：

```
[output omitted]
Licensed features for this platform:
Maximum VLANs : 50
Inside Hosts : Unlimited
Failover : Active/Standby
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 0
Carrier : Enabled
AnyConnect Premium Peers : 250
AnyConnect Essentials : Disabled
Other VPN Peers : 250
Total VPN Peers : 250
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 500
Botnet Traffic Filter : Enabled
Cluster : Disabled
```

如果此功能未启用，则需要与许可证团队合作以获取适当的许可证。现在，您已确认您的ASA支持VPN电话，您可以开始配置。

注意：配置部分中带下划线的所有项目都是可配置名称，可以更改。大多数这些名称在配置中的其他位置被引用，因此记住在这些部分（组策略、隧道组等）中使用的名称非常重要，因为您以后需要这些名称。

步骤2.为VPN客户端创建IP地址池。这类似于DHCP池，即当IP电话连接到ASA时，它从该池接收IP地址。在ASA上，可以使用以下命令创建池：

```
ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254 mask 255.255.255.0
```

此外，如果您喜欢不同的网络或子网掩码，也可以更改。创建池后，您需要配置组策略（ASA和IP电话之间连接的一组参数）：

```
group-policy vpn-phone-policy internal
```

```
group-policy vpn-phone-policy属性
```

```
split-tunnel-policy tunnelall
```

```
vpn-tunnel-protocol ssl-client
```

步骤3.如果AnyConnect尚未启用，则需要启用它。为此，您需要知道外部接口的名称。通常，此接口命名为**outside**（如代码片断所示），但是它是可配置的，因此请务必确认您具有正确的接口。请运行**show ip**以查看接口列表：

```
sckiewer-ASAv# show ip
System IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
```

```
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
Current IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
```

在此环境中，外部接口命名为**outside**，因此这些命令在该接口上启用AnyConnect。

webvpn

启用外部

```
anyconnect enable
```

步骤4.配置新隧道组，以便将之前创建的组策略应用于特定URL上连接的任何客户端。 请注意对您之前在代码片断的第3行和第4行中创建的IP地址池和组策略名称的引用。 如果修改了IP地址池或组策略的名称，则需要使用修改后的名称替换不正确的值：

```
tunnel-group vpn-phone-group type remote-access
tunnel-group vpn-phone-group general-attributes
  address-pool vpn-phone-pool
  default-group-policy vpn-phone-policy
tunnel-group vpn-phone-group webvpn-attributes
  认证证书
  group-url https://asav.sckiewer.lab/phone enable
```

可以使用IP地址，而不是组URL的名称。 如果电话无法访问可解析ASA的完全限定域名(FQDN)的DNS服务器，则通常会执行此操作。 此外，您可以看到此示例使用基于证书的身份验证。 您也可以选择使用用户名/密码身份验证，但ASA有更多要求不在本文档的范围内。

在本示例中，DNS服务器有A记录**asav.sckiewer.lab - 172.16.1.250**，从show ip输出中可以看到，172.16.1.250在名为**outside**的接口上配置。 因此配置为：

```
crypto ca trustpoint asa-identity-cert
```

注册自

```
subject-name CN=asav.sckiewer.lab
```

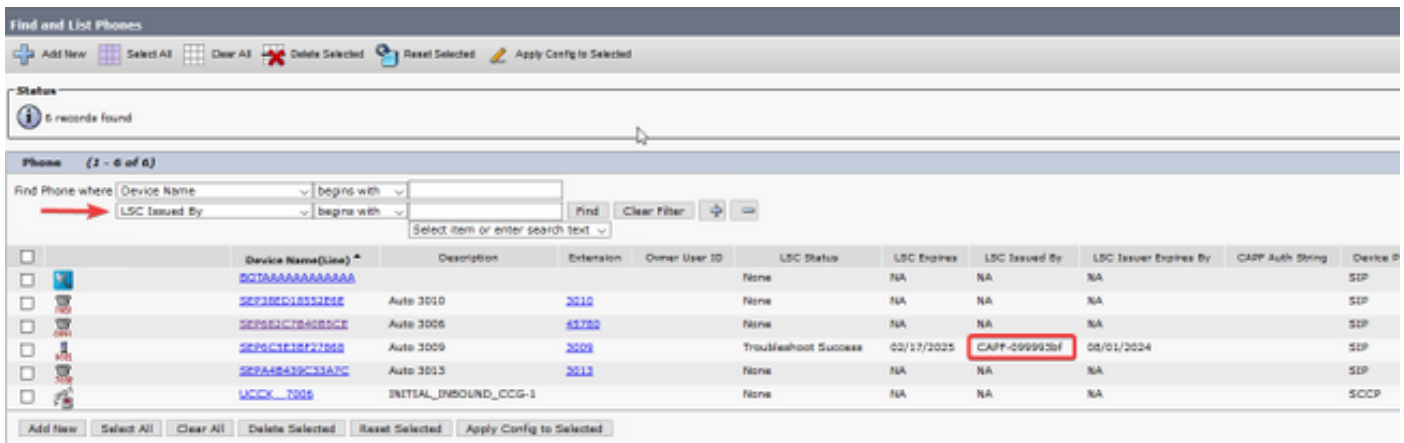
```
crypto ca enroll asa-identity-cert
```

```
ssl trust-point asa-identity-cert outside
```

需要注意的几点：

1. 已创建名为**asa-identity-cert**的新信任点，并且已对其应用了主题名称。 这会导致从此信任点生成的证书使用指定的使用者名称
2. 接下来，使用“crypto ca enroll **asa-identity-cert**”命令，ASA可以生成自签名证书并将其保存到该信任点
3. 最后，ASA将信任点中的证书呈现给连接到外部接口的任何设备

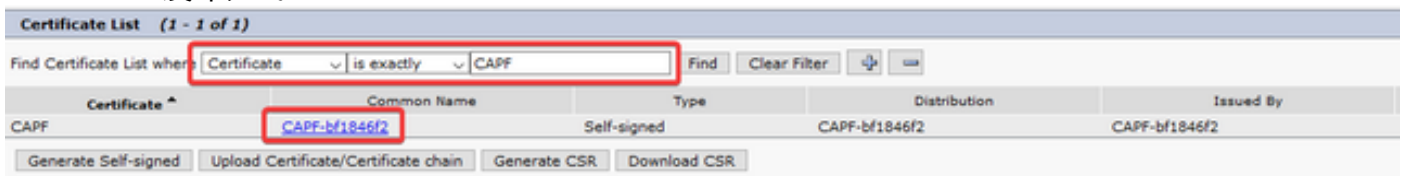
步骤5.创建必要的信任点，以允许ASA信任IP电话的证书。 首先，您需要确定您的IP电话是使用制造商安装的证书(MIC)还是本地有效证书(LSC)。 默认情况下，除非在所有电话上安装LSC，否则所有电话都使用其MIC进行安全连接。 在CUCM 11.5.1及更高版本中，您可以在**Unified CM Administration > Device > Phone**中运行搜索，以查看LSC是否已安装，而较旧版本的CUCM要求您实际检查每部电话的安全设置。 在CUCM 11.5.1中，请注意，您需要将过滤器（或更改默认过滤器）添加到LSC Issued By。 LSC Issued By列中有**NA**的设备使用MIC，因为它们没有安装LSC。



如果您的电话看起来与图像中突出显示的电话相似，则需要将CUCM发布者的CAPF证书上传到ASA，以便ASA验证电话的证书以进行安全连接。 如果要使用未安装LSC的设备，则需要将思科制造证书上传到ASA。 这些证书可在CUCM发布服务器上的Cisco Unified OS Administration > Security > Certificate Management中找到：

注意：您可以看到，其中一些证书位于多个信任存储（CallManager-trust和CAPF-trust）中。从哪个信任库下载证书并不重要，只要您确保选择具有这些确切名称的证书。

- Cisco_Root_CA_2048 < MIC SHA-1 Root
- Cisco_Manufacturing_CA < MIC SHA-1中间
- Cisco_Root_CA_M2 < MIC SHA-256根
- Cisco_Manufacturing_CA_SHA2 < MIC SHA-256中间
- CUCM发布方的CAPF < LSC



在MIC方面，79xx和99xx系列等较旧的电话型号使用SHA-1证书链，而88xx系列等较新的电话型号则使用SHA-256证书链。 您的电话使用的证书链需要上传到ASA。

获得所需的证书后，可以使用以下命令创建信任点：

crypto ca trustpoint cert1

注册终端

crypto ca authenticate cert1

第一个命令创建名为cert1的信任点，crypto ca authenticate命令允许您将base64编码的证书粘贴到CLI中。 您可以根据需要多次运行这些命令以在ASA上获取适当的信任点，但请确保为每个证书使用新的信任点名称。

步骤6.发出以下命令获取ASA身份证书的副本：

crypto ca export asa-identity-cert identity-certificate

这会导出名为asa-identity-cert的信任点的身份证书。 请务必调整名称，使其与您在步骤4中创建的信任点匹配。

以下是ASA的完整实验配置：

```
ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254 mask 255.255.255.0

group-policy vpn-phone-policy internal
group-policy vpn-phone-policy attributes
    split-tunnel-policy tunnelall
    vpn-tunnel-protocol ssl-client

webvpn
    enable outside
    anyconnect enable

tunnel-group vpn-phone-group type remote-access
tunnel-group vpn-phone-group general-attributes
    address-pool vpn-phone-pool
    default-group-policy vpn-phone-policy

tunnel-group vpn-phone-group webvpn-attributes
    authentication certificate
    group-url https://asav.sckiewer.lab/phone enable

ssl trust-point asa-identity-cert outside
```

此时，ASA配置已完成，您可以继续配置CUCM。您需要您刚收集的ASA证书副本和在隧道组部分配置的URL。

CUCM 配置

步骤1.在CUCM上，导航至Cisco Unified OS Administration > Security > Certificate Management，并将ASA证书作为phone-vpn-trust上传。

The screenshot shows the 'Certificate List' interface in Cisco Unified OS Administration. At the top, there are four icons: 'Generate Self-signed', 'Upload Certificate/Certificate chain', 'Download CTL', and 'Generate CSR'. Below this is a 'Status' section indicating '1 records found'. The main section is titled 'Certificate List (1 - 1 of 1)'. It features a search bar with the text 'Find Certificate List where Certificate begins with phone-vpn'. Below the search bar is a table with columns: 'Certificate', 'Common Name', and 'Type'. The table contains one row: 'Phone-VPN-trust' with 'asav.sckiewer.lab' in the 'Common Name' column and 'Self-signed' in the 'Type' column. This row is highlighted with a red border. Below the table are four buttons: 'Generate Self-signed', 'Upload Certificate/Certificate chain', 'Download CTL', and 'Generate CSR'.




步骤2.完成此操作后，导航至Cisco Unified CM Administration > Advanced Features > VPN > VPN Profile并创建新配置文件。本部分没有对错，了解每个设置的用途非常重要。

1. **启用自动网络检测**(Auto Network Detect) — 启用此功能后，电话会在打开电源时ping其TFTP服务器。如果收到对此ping的响应，则不启用VPN。如果电话未收到对此ping的响应，则启用VPN。启用此设置后，无法手动启用VPN。
2. **主机ID检查** — 启用此功能后，电话会从其配置文件(本文档中使用


<https://asav.sckiewer.lab/phone>)检查VPN URL，并确保主机名或FQDN与ASA提供的证书中的公用名(CN)或SAN条目匹配。

3. **身份验证方法** — 控制用于连接ASA的身份验证方法类型。在本文档的配置示例中，使用基于证书的身份验证。
4. **密码持久性** — 如果启用此功能，则客户端的密码将存储在电话中，直到尝试登录失败、客户端手动清除密码或电话重置为止。

VPN Profile Configuration

Save  Delete  Copy  Add New

Status

 Status: Ready

VPN Profile Information

Name*

Description

Enable Auto Network Detect

Tunnel Parameters

MTU*

Fail to Connect*

Enable Host ID Check

Client Authentication

Client Authentication Method*

Enable Password Persistence

Save Delete Copy Add New

步骤3.接下来，导航至Cisco Unified CM管理>高级功能>VPN > VPN网关。您需要确保VPN网关URL与ASA配置匹配，并确保证书从顶部框移动到底部框，如图所示：

VPN Gateway Configuration

Save

Status
Status: Ready

VPN Gateway Information
VPN Gateway Name*
VPN Gateway Description
VPN Gateway URL*

VPN Gateway Certificates
VPN Certificates in your Truststore
VPN Certificates in this Location*

步骤4.保存后，您需要导航到Cisco Unified CM Administration > Advanced Features > VPN > VPN Group，并将您创建的网关移到“Selected VPN Gateways in this VPN Group”框：

VPN Group Configuration

Save

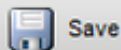
Status
Status: Ready

VPN Group Information
VPN Group Name*
VPN Group Description

VPN Gateway Information
All Available VPN Gateways
Selected VPN Gateways in this VPN Group:

步骤5.配置VPN设置后，您需要导航至Cisco Unified CM Administration > Device > Device Settings > Common Phone Profile。在此，您必须复制所需VPN电话使用的配置文件，重命名它，然后选择VPN组和VPN配置文件，然后保存新配置文件：

Common Phone Profile Configuration



Save

Status



Status: Ready

Common Phone Profile Information

Name*	<input type="text" value="Standard Common Phone Profile - VPN_Auto-On"/>
Description	<input type="text" value="Standard Common Phone Profile - VPN_Auto-On"/>
Local Phone Unlock Password	<input type="text"/>
DND Option*	<input type="text" value="Ringer Off"/>
DND Incoming Call Alert*	<input type="text" value="Beep Only"/>
Feature Control Policy	<input type="text" value="< None >"/>
Wi-Fi Hotspot Profile	<input type="text" value="< None >"/> View Details

Enable End User Access to Phone Background Image Setting

Secure Shell Information

Secure Shell User	<input type="text"/>
Secure Shell Password	<input type="text"/>

Phone Personalization Information

Phone Personalization*	<input type="text" value="Default"/>
Always Use Prime Line*	<input type="text" value="Default"/>
Always Use Prime Line for Voice Message*	<input type="text" value="Default"/>
Services Provisioning*	<input type="text" value="Default"/>

VPN Information

VPN Group	<input type="text" value="VPN_Group_1"/>
VPN Profile	<input type="text" value="VPN_Profile"/>

步骤6.最后，您需要将此新配置文件应用到您的电话，然后在电话处于内部网络时重置该电话。这允许电话接收所有新配置，如ASA证书哈希和VPN URL。

注意：在测试电话之前，您需要确保电话已配置“备用TFTP”服务器。由于ASA不为电话提供选项150，因此需要在电话上手动配置TFTP IP。

步骤7.测试VPN电话，并验证它是否能成功连接到ASA并注册。您可以验证隧道在ASA上是否已启用，**show vpn-sessiondb anyconnect:**

```
sckiewer-ASAv# show vpn-sessiondb anyconnect
Session Type: AnyConnect
Username      : CP-8841-SEP682C7B40B5CE
Index        : 3
Assigned IP   : 10.10.1.131      Public IP    : 192.168.1.52
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption    : AnyConnect-Parent: (1)AES256 SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 4275771          Bytes Rx     : 32476192
Group Policy  : VPN-Phone        Tunnel Group : VPN-Phone
Login Time    : 01:07:39 UTC Fri Mar 27 2020
Duration      : 4d 1h:56m:42s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A              VLAN         : none
Audt Sess ID  : 0e3051fa000030005e7d51db
Security Grp  : none
```

故障排除

要收集的数据

要排除VPN电话问题，建议使用以下数据：

- ASA调试：logging buffered debuglogging debug-tracedebug crypto ca transactions 255debug crypto ca messages 255debug crypto ca 255debug webvpn 255debug webvpn anyconnect 255
- 电话控制台日志(或PRT (如果电话支持) — 此处提供[详细信息](#))

在启用调试后重现问题后，您可以使用此命令查看输出，因为调试输出始终包含711001:

```
show log | i 711001
```

常见问题

注意：就本节而言，日志片段来自8861电话，因为这是部署为VPN电话的较常见电话系列之一。请记住，其他型号可以在日志中写入不同的消息。

更新ASA自签名身份证书

在ASA身份证书过期之前，需要生成新证书并将其推送到电话。要在不影响VPN电话的情况下执行此操作，请使用以下流程：

步骤1.为新身份证书创建新信任点：

```
crypto ca trustpoint asa-identity-cert-2
```

注册自

```
subject-name CN=asav.sckiewer.lab
```

crypto ca enroll asa-identity-cert-2

步骤2.此时，您将拥有ASA的新身份证书，但尚未在任何接口上使用。您需要导出此新证书并将其上传到CUCM:

crypto ca export asa-identity-cert-2 identity-certificate

步骤3.获得新的身份证书后，在Cisco Unified OS Administration > Security > Certificate Management > Upload上将其作为电话 — VPN-trust上传到您的CUCM节点之一。

注意：当前电话VPN信任证书只存在于最初上传到的CUCM节点上（它不会自动传播到其他节点，如某些证书）。如果CUCM版本受CSCuo58506[影响](#)，则必须将新的ASA证书上传到其他节点。

步骤4.将新证书上传到集群中的任何节点后，在CUCM发布服务器上导航至Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway

步骤5.选择适当的网关。

步骤6.在顶部框中选择证书（这是您刚上传的证书），然后选择向下箭头将其移至底部（这允许TFTP将该证书添加到VPN电话的配置文件中），并选择Save。

步骤7.完成后，重置所有VPN电话。在此过程中，ASA仍显示旧证书，因此电话可以连接，但是，它们会获取包含新证书和旧证书的新配置文件。

步骤8.现在，您可以将新证书应用到ASA。为此，您需要新信任点的名称和外部接口的名称，然后使用该信息运行此命令：

ssl trust-point asa-identity-cert-2 outside

注意：您可以在浏览器中导航至webvpn URL，以验证ASA是否提供新证书。由于外部电话必须可以公开访问该地址才能访问该地址，因此您的PC也可以访问该地址。然后，您可以检查ASA向您的浏览器提供的证书，并确认它是新证书。

步骤9.将ASA配置为使用新证书后，重置测试电话并验证它是否能够连接到ASA并注册。如果电话成功注册，则您可以重置所有电话并验证它们是否能够连接到ASA并注册。这是推荐的流程，因为连接到ASA的电话在证书更改后仍保持连接。如果先在一部电话上测试证书更新，则配置问题影响大量电话的风险会降低。如果第一个VPN电话无法连接到ASA，则可以从电话和/或ASA收集日志以排除故障，而其他电话仍保持连接。

步骤10.在您验证电话能够连接并注册新证书后，可以从CUCM中删除旧证书。

ASA选择椭圆曲线(EC)密码

自9.4(x)起，ASA支持椭圆曲线(EC)加密，因此，在ASA升级到9.4(x)或更高版本后，通常会看到以前工作的VPN电话出现故障。这是因为ASA现在在与较新电话型号的TLS握手期间选择EC密码。通常，有一个RSA证书与电话连接的接口关联，因为以前的ASA版本不支持EC。此时，由于ASA已选择EC密码，因此无法使用RSA证书进行连接，因此它会生成并发送电话临时自签名证书，该证书由EC算法而非RSA创建。由于电话无法识别此临时证书，因此连接失败。您可以在88xx电话日志中验证这一点非常简单。

```
2101 NOT Mar 30 12:23:21.331861 (393:393) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
2102 NOT Mar 30 12:23:21.331871 (393:393) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
```

电话日志显示ASA为此连接选择了EC密码，因为“新密码”行包含导致连接失败的EC密码。

在选择AES的场景中，您将看到：

```
2691 NOT Mar 30 12:18:19.016923 (907:907) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
2690 NOT Mar 30 12:18:19.016943 (907:907) VPNC: -protocol_handler: new cipher -> AES256-
SHA:AES128-SHA
```

有关此项的详细信息，请点击[CSCuu02848](#)。

解决方法是在ASA上为您的电话使用的TLS版本禁用EC密码。有关每个电话型号支持的TLS版本的详细信息，请访问：

Table 6 lists the TLS versions supported by the Cisco IP phones.

Table 6. TLS version support

Version	Phone Models			
	7900	6900, 8900, 9900	7811, 7821, 7841, 7861	8811, 8821, 8841, 8845, 8851, 8861, 8865
TLS 1.0	Yes	Yes	Yes	Yes
TLS 1.2	No	No	Yes	Yes
Disable TLS 1.0 and TLS 1.1 with https for web access*	No	No	Yes	Yes
Selectively Disable TLS cipher suites used by TLS connection or handshake**	No	No	Yes	Yes

* With 12.1 firmware
 ** With 12.5 firmware

<https://www.cisco.com/c/dam/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-c11-739097.pdf>

一旦您知道哪些TLS版本与您的环境相关，您就可以在ASA上运行以下命令，为这些版本禁用EC密码：

```
ssl cipher tlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
ssl cipher tlsv1.1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
ssl cipher dtlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
```

请记住，IP电话默认使用DTLS（数据报传输层安全），因此您需要为DTLS运行密码语句，并为电话运行相关TLS版本。此外，了解这些更改是ASA上的全局更改非常重要，因此它们可防止使用这些TLS版本的任何其他AnyConnect客户端协商EC密码。

DTLS连接失败

在某些情况下，VPN电话无法建立与具有DTLS的ASA的连接。如果电话尝试使用DTLS但失败，则电话继续反复尝试DTLS，但未成功，因为它知道DTLS已启用。您将在88xx电话日志中看到以下内容：

```
3249 ERR Mar 29 15:22:38.949354 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert:
fatal:illegal parameter
3250 NOT Mar 29 15:22:38.951428 (385:385) VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000
status: 0x0 error: 0x0
3251 ERR Mar 29 15:22:38.951462 (385:385) VPNC: -alert_err: DTLS write alert: code 47, illegal
parameter
3252 ERR Mar 29 15:22:38.951489 (385:385) VPNC: -create_dtls_connection: SSL_connect ret -1,
error 1
3253 ERR Mar 29 15:22:38.951506 (385:385) VPNC: -DTLS: SSL_connect: SSL_ERROR_SSL (error 1)
3254 ERR Mar 29 15:22:38.951552 (385:385) VPNC: -DTLS: SSL_connect: error:140920C5:SSL
routines:ssl3_get_server_hello:old session cipher not returned
3255 ERR Mar 29 15:22:38.951570 (385:385) VPNC: -create_dtls_connection: DTLS setup failure,
cleanup
3256 WRN Mar 29 15:22:38.951591 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert:
warning:close notify
3257 ERR Mar 29 15:22:38.951661 (385:385) VPNC: -do_dtls_connect: create_dtls_connection failed
3258 ERR Mar 29 15:22:38.951722 (385:385) VPNC: -protocol_handler: connect: do_dtls_connect
failed
3259 WRN Mar 29 15:22:38.951739 (385:385) VPNC: -protocol_handler: connect : err: SSL success
DTLS fail
```

这可能是由于“[ASA选择椭圆曲线\(EC\)密码](#)”部分中提及的相同问题导致的，因此您必须确保为DTLS禁用了EC密码。除此之外，您可以完全禁用DTLS，这会强制VPN电话使用TLS。这并不理想，因为它意味着所有流量都将使用TCP而非UDP，这会增加一些开销。但是，在某些情况下，这是一个很好的测试，因为它至少确认了大多数配置都正常，并且问题特定于DTLS。如果要测试此项，最好在组策略级别执行，因为管理员通常对VPN电话使用唯一的组策略，因此这样我们就可以测试更改而不影响其他客户端。

group-policy vpn-phone-policy属性
webvpn
anyconnect ssl dtls none

另一个可能阻止成功DTLS连接的常见配置问题是电话无法使用同一密码建立TLS和DTLS连接。日志摘录示例：

```
%%%% TLS Ciphers Offered
3905 NOT Apr 01 20:14:22.741838 (362:362) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA

%%%% DTLS Ciphers Offered
4455 NOT Apr 01 20:14:23.405417 (362:362) VPNC: -process_connect: x-dtls-ciphersuite: AES128-SHA
4487 NOT Apr 01 20:14:23.523994 (362:362) VPNC: -create_dtls_connection: cipher list: AES128-SHA

%%%% DTLS connection failure
4496 WRN Apr 01 20:14:53.547046 (362:474) VPNC: -vpnc_control: conn timer expired at:1585772093,
to abort connect
4497 NOT Apr 01 20:14:53.547104 (362:474) VPNC: -abort_connect: in dtls setup phase
```

您可以从代码片断的第一行看到提供的TLS密码。选择了两端支持的最安全选项（日志不显示选择，但是，您可以推断它至少是来自日志片段的AES-256）。您还可以看到仅提供DTLS密码的是AES128。由于所选TLS密码对DTLS不可用，连接失败。此场景中的解决方法是确保ASA配置允许将相同的密码用于TLS和DTLS。

证书更新后电话无法连接到ASA

在CUCM上将新的ASA身份证书作为phone-vpn-trust上传，以便电话可以获取此新证书的哈希值，这一点非常重要。如果未遵循此过程，则在更新后以及下次VPN电话尝试连接到ASA时，电话将显示不信任的证书，因此连接失败。ASA证书更新后，可能会在几天或几周内发生这种情况，因为当证书更改时，电话不会断开连接。只要ASA继续从电话接收keepalive，VPN隧道就会保持运行。因此，如果您确认ASA证书已更新，但新证书未首先放在CUCM上，则您有两个选项：

1. 如果旧ASA身份证书仍然有效，请将ASA恢复为旧证书，然后按照本文档中提供的过程更新证书。如果已生成新证书，可跳过证书生成部分。
2. 如果旧ASA身份证书已过期，您需要将新ASA证书上传到CUCM，并将电话重新连接到内部网络，以接收具有新证书哈希值的更新配置文件。

电话无法通过DNS解析ASA URL

在某些情况下，管理员使用主机名而不是IP地址配置VPN URL。完成此操作后，电话需要有DNS服务器才能将名称解析为IP地址。在代码片断中，您可以看到电话尝试使用其两台DNS服务器192.168.1.1和192.168.1.2解析域名，但没有收到响应。30秒后，电话将打印“DnsLookupErr：”

```
3816 NOT Mar 3 15:38:03.819168 VPNC: -do_login: URL -> https://asav.sckiewer.lab/phone
...
3828 INF Mar 3 15:38:03.834915 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3829 INF Mar 3 15:38:03.835004 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3830 INF Mar 3 15:38:03.835030 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3831 INF Mar 3 15:38:17.845305 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3832 INF Mar 3 15:38:17.845352 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3833 INF Mar 3 15:38:17.845373 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3834 INF Mar 3 15:38:31.854834 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3835 INF Mar 3 15:38:31.854893 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3836 INF Mar 3 15:38:31.855213 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3837 ERR Mar 3 15:38:32.864376 VPNC: -parse_url: gethostbyname failed <asav.sckiewer.lab>
3838 NOT Mar 3 15:38:32.864435 VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000 status:
0x0 error: 0x0
3839 ERR Mar 3 15:38:32.864464 VPNC: -do_login: parse URL failed ->
https://asav.sckiewer.lab/phone
3840 NOT Mar 3 15:38:32.864482 VPNC: -vpn_stop: de-activating vpn
3841 NOT Mar 3 15:38:32.864496 VPNC: -vpn_set_auto: auto -> auto
3842 NOT Mar 3 15:38:32.864509 VPNC: -vpn_set_active: activated -> de-activated
3843 NOT Mar 3 15:38:32.864523 VPNC: -set_login_state: LOGIN: 1 (TRYING) --> 3 (FAILED)
3844 NOT Mar 3 15:38:32.864538 VPNC: -set_login_state: VPNC : 1 (LoggingIn) --> 3 (LoginFailed)
3845 NOT Mar 3 15:38:32.864561 VPNC: -vpnc_send_notify: notify type: 1 [LoginFailed]
3846 NOT Mar 3 15:38:32.864580 VPNC: -vpnc_send_notify: notify code: 32 [DnsLookupErr]
3847 NOT Mar 3 15:38:32.864611 VPNC: -vpnc_send_notify: notify desc: [url hostname lookup err]
```

这通常表示以下情况之一：

1. 电话的DNS服务器无效
2. 电话未通过DHCP接收DNS服务器或未手动配置

要解决此问题，有两个选项：

1. 检查电话上的配置，确保在电话外部时从DHCP服务器接收DNS服务器，并/或验证电话的DNS服务器可以解析ASA配置中使用的名称
2. 将ASA配置和CUCM中的URL更改为IP地址，以便无需DNS

电话不启用VPN

如本文前面所述，自动网络检测使电话ping TFTP服务器并检查响应。如果电话在内部网络中，则TFTP服务器可在没有VPN的情况下访问，因此当电话收到对ping的响应时，它不会启用VPN。当电话不在内部网络中时，ping操作会失败，因此电话将启用VPN并连接到ASA。请记住，客户端的家庭网络可能不会配置为通过DHCP为电话提供选项150，而且ASA也不能提供选项150，因此VPN电话需要“备用TFTP”。

在日志中，您需要验证以下几项：

1. 电话是否对CUCM TFTP服务器IP执行ping操作？
2. 电话是否收到对ping的响应？
3. 电话在未收到对ping的响应后是否启用VPN？

请务必按此顺序查看这些项目。在电话对错误的IP执行ping操作并收到响应的情况下，在ASA上启用调试将毫无意义，因为电话将不启用VPN。按此顺序验证这三件事，以便防止不必要的日志分析。如果ping失败，并且VPN在之后启用，您将在88xx电话日志中看到以下内容：

```
5645 NOT Mar 27 11:32:34.630109 (574:769) JAVA-vpnAutoDetect: ping time out
5647 DEB Mar 27 11:32:34.630776 (710:863) JAVA-configmgr MQThread|cip.vpn.VpnStateHandler:? -
VpnStateHandler: handleVPN_ENABLED_STATE()
```

电话注册但无法显示呼叫历史记录

验证电话是否启用了备用TFTP并配置了正确的TFTP IP。备用TFTP是VPN电话的要求，因为ASA不能提供选项150。

相关信息

- [技术支持和文档 - Cisco Systems](#)